(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月11 日 (11.08.2005)

PCT

(10) 国際公開番号
WO 2005/074185 A1

(51) 国際特許分類[7]: H04L 9/08

(21) 国際出願番号: PCT/JP2005/001359

(22) 国際出願日: 2005 年1 月31 日 (31.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-025386 2004 年2 月2 日 (02.02.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 野仲 真佐男 (NONAKA, Masao). 布田 裕一 (FUTA, Yuichi). 大森 基司 (OHMORI, Motoji). 山田 茂 (YAMADA, Shigeru). 井上 哲也 (INOUE, Tetsuya). 熊崎 洋児 (KUMAZAKI, Yoji). 黒岩 渉 (KUROIWA, Wataru). 大井 伸一 (OI, Shin'ichi). 吉田 治 (YOSHIDA, Osamu).

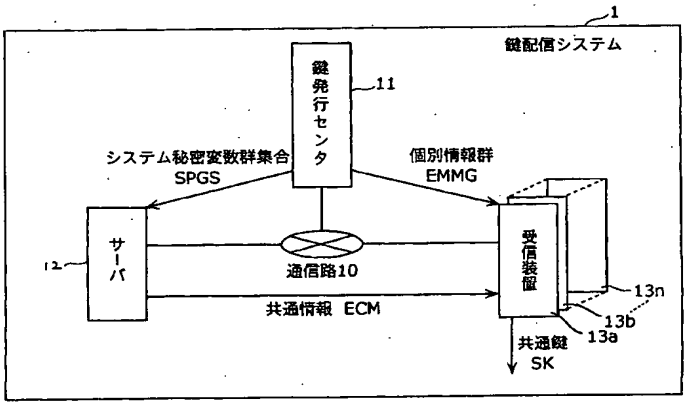
(74) 代理人: 新居 広守 (NII, Hiromori); 〒5320011 大阪府大阪市淀川区西中島３丁目１１番２６号 新大阪末広センタービル３Ｆ 新居国際特許事務所内 Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: KEY DISTRIBUTION SYSTEM

(54) 発明の名称: 鍵配信システム



1.. KEY DISTRIBUTION SYSTEM
11.. KEY ISSUANCE CENTER
SPGS.. SYSTEM PRIVATE VARIABLE GROUP SET
EMMG.. INDIVIDUAL INFORMATION GROUP
12.. SERVER
10.. COMMUNICATION PATH
ECM.. COMMON INFORMATION
13a.. RECEIVER DEVICE
SK.. SHARED KEY

(57) Abstract: It was not possible to determine a clone source of unauthorized receiver devices. A key distribution system (1) of the present invention comprises a communication path (10), a key issuance center (11), a server (12), and a plurality of receiver devices (13a-13n). The key issuance center (11) distributes, to the server (12), a system private variable group set (SPGS) that is information necessary for distributing a shared key (SK) to the receiver devices (13a-13n), while distributing, to the plurality of receiver devices (13a-13n), an individual information group (EMMG) necessary for receiving the shared key (SK) from the server (12). The server (12) produces the shared key (SK), also produces, based

[続葉有]

WO 2005/074185 A1

SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

on the shared key (SK) and system private variable group set (SPGS), a common information (ECM), and then distributes the common information (ECM) to the plurality of receiver devices (13a-13n). The receiver devices (13a-13n) acquire, based on the individual information group (EMMG) and common information (ECM), the shared key (SK) and output it to the exterior.

(57) 要約: 不正な受信装置のクローン元を特定することが出来なかった。本発明にかかる鍵配信システム１は、通信路１０と、鍵発行センタ１１と、サーバ１２と、複数の受信装置１３ａ～１３ｎから構成される。鍵発行センタ１１は共有鍵ＳＫを受信装置１３ａ～１３ｎへ配信するのに必要な情報であるシステム秘密変数群集合ＳＰＧＳをサーバ１２へ、サーバ１２から共有鍵ＳＫを受信するのに必要な個別情報群ＥＭＭＧを複数の受信装置１３ａ～１３ｎへ配信する。サーバ１２は、共有鍵ＳＫを生成し、その共有鍵ＳＫ及びシステム秘密変数群集合ＳＰＧＳを基に共通情報ＥＣＭを生成し、その共通情報ＥＣＭを複数の受信装置１３ａ～１３ｎへ配信する。受信装置１３ａ～１３ｎは、個別情報群ＥＭＭＧ及び共通情報ＥＣＭを基に、共有鍵ＳＫを取得し、外部へ出力する。